A Process Mining Tool for Supporting IoT Security

Adrien Hemmer, Remi Badonnel, Jérôme François, Isabelle Chrisment

A Process Mining Tool for Supporting IoT Security

Adrien Hemmer, Rémi Badonnel, Jérôme François and Isabelle Chrisment
Inria Nancy Grand Est - LORIA
Campus Scientifique, 54600 Villers-les-Nancy, France
{adrien.hemmer, remi.badonnel, jerome.francois, isabelle.chrisment}@inria.fr

***Abstract*—The development of the Internet has been characterized by a growing interest for the Internet-of-Things (IoT). In particular, connected devices are integrated to other Internet resources (such as cloud resources) to elaborate value-added services. However, they pose important challenges with respect to security management due to their heterogeneity, their distribution, and their limited resources. In this demonstration, we present a process mining toool for supporting IoT security. This tool is capable to automate the detection of misbehaviours and attacks in large and heterogeneous IoT infrastructures, based on process mining techniques combined with normalization and clustering data pre-processing. We detail the different building blocks of this tool provided into a docker container, and illustrate its operations with different scenarios.**

I. Introduction

The Internet-of-Things (IoT) has grown in importance and maturity in a large variety of application domains, such as home automation systems, healthcare applications and industry 4.0 infrastructures. The complexity of these systems involving IoT devices is often under-estimated [1], and introduces new challenges from a security management viewpoint [2]. IoT-based systems are an attractive target for security attacks. This phenomenon can be explained by several factors [3], including the complexity of these systems, that can be composed of multiple and distributed devices, and the limited ressources (memory, CPU, battery) of these devices. These ones are often subject of naïve weaknesses such as default credentials, poor maintenance and misconfigurations [2] [4]. In addition, the heterogeneity of IoT protocols and devices make the security management tasks more complicated. The vulnerabilities of IoT devices have an impact that goes beyond the Internet-of-Things, and may affect more elaborated services built on top of these resources.

Solutions have already been proposed in the litterature to address security issues due to the Internet-of-things and can be distinguished into two main categories. First, security approaches against external attacks that rely on authentication methods based on cryptographic techniques [5], where the attacker tries to acquire rights and permissions over the IoT-based system. Secondly, security approaches against internal attacks that may typically rely on misbehaviour detection techniques, considering that the attackers may already have permissions over the IoT-based system [6].

We propose in this demonstration a process mining tool for supporting and automating IoT security in different application domains, which may include both internal and external attacks. This tool is capable to deal with heterogeneous IoT-based systems through the analysis of networking and application data coming from various sources. It is an implementation of the process mining approach presented in [7].

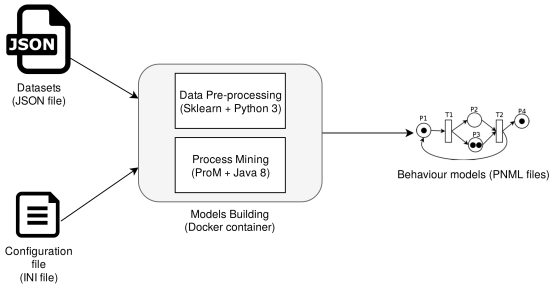

Fig. 1. Model building phase of our process mining tool

The remainder of the paper is organized as follows. Section II describes the proposed tool for automating IoT security, based on process mining techniques combined with normalization and clustering data pre-processing. Section III details the scenarios and functionalities of the tool that will be showcased during the demonstration.

II. Process mining tool

The proposed tool has been designed to automate IoT security and supports the detection of misbehaviours and potential attacks in IoT-based systems that may include heterogeneous protocols and devices. The tool is embedded into a docker container, and provides dedicated interfaces in order to facilitate its integration with other security management solutions. The tool takes as inputs a large variety of datasets that may come from several IoT application domains, and supports both continuous and categorical data that are not processed in the same manner for performance purposes. The tool operates according to two main phases: a model building phase that combines data pre-processing with process mining, and an evaluation phase that combines data pre-processing with conformance checking.

The first phase, called model building is illustrated on Figure 1. It permits to automatically generate behaviour models from IoT datasets using process mining, and takes into account configuration parameters defined by users (including normalization and clustering parameterizations). It relies on

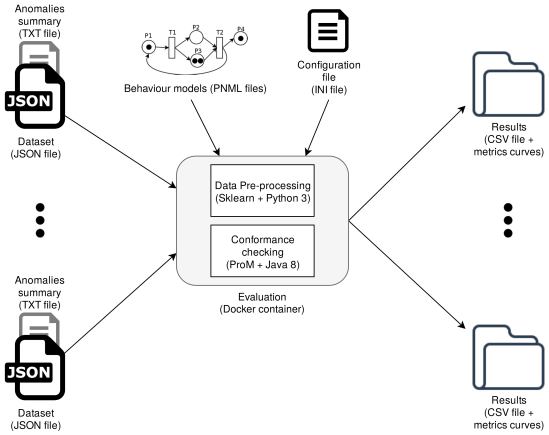

Fig. 2. Evaluation phase of our process mining tool

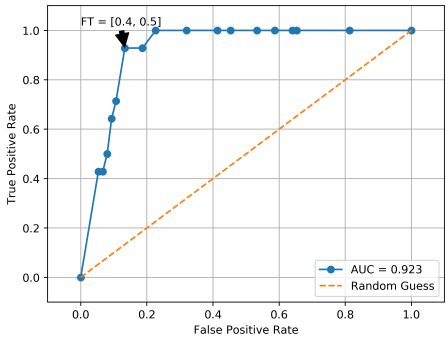

Fig. 3. Example of a Roc curve generated with the process mining tool

two main building blocks. The first one, called data pre-processing, has been developed in Python 3.6. It normalizes, then clusterizes the datasets, using the Sklearn library [8]. The clustering only concerns continuous data in order to group them into dedicated clusters. The data pre-processing permits to characterize and minimize the number of states of the IoT-based system. The second building block, called process mining, has been developed in Java 8. It is capable to generate Petri net models from pre-processed data, based on the the ProM version 6.8 library [9].

The second phase, called evaluation phase, is depicted on Figure 2. It permits to automatically detect misbehaviours and potential attacks from the generated behaviour models, but also to quantify the detection performances. It is composed of two main building blocks. The first one, corresponding to the data pre-processing, is quite similar to the model building one. It consists into normalizing considered datasets, and clusterizing the continuous data before using them with the categorical features, in order to characterize the system states. A binding process permits to ensure the same parameterizations of normalization and clustering techniques, depending on the nature of the datasets. The pre-processed data are then replayed on the behaviour models, using a second building block, called conformance checking. This one quantifies potential deviations with the ProM library, and detects misbehaviours over the IoT-based system. The evaluation phase and the model building phase correspond both to the fully automated processes.

III. The Demonstration

In this demonstration, we will present our process mining tool for supporting IoT security, by showcasing both the model building phase and the evaluation phase. We will consider experimental datasets coming from different scenarios in IoT-based systems, in particular connected/smart vehicles and industry 4.0. For connected vehicles, the datasets will include vehicle-to-everything (V2X) communication data providing different parameters such as the vehicle speed and its steering angle. For the industry 4.0, we will focus on datasets coming from a plastic molding process, including temperature sensors at several locations in the system, and pressure sensors inside each relevant piston. We will demonstrate for each scenario, the configuration and operation of our automated solution. We will show the model building phase with the considered configuration files, the experimental datasets, and the generation of behaviour models as Petri nets. We will also show the evaluation phase with the experimental datasets, and the detection of misbehaviours. In that context, we will generate automatically with the tool, the performances of the detection based on ROC (Receiver Operating Characteristic) curves, such as the one illustrated on Figure 3, and quantify the processing time with a variety and heterogeneity of datasets.

Acknowledgment

This work has been partially supported by the SecureIoT project, funded by the European Union's Horizon 2020 research and innovation programme under grant agreement no. 779899.

References

[1] K. Delaney and E. Levy, "Connected Futures Cisco Research: IoT Value: Challenges, Breakthroughs, and Best Practices." Cisco System Report, May 2017.

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the Mirai Botnet," in *Proceedings of the USENIX Security Symposium*, 2017, pp. 1092–1110.

[3] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer*, vol. 50, no. 02, pp. 76–79, feb 2017.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[5] M. Pahl and L. Donini, "Securing IoT Microservices with Certificates," in *Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*, April 2018, pp. 1–5.

[6] F. Bezerra, J. Wainer, and W. M. P. Aalst, "Anomaly Detection Using Process Mining," vol. 29, 01 2009, pp. 149–161.

[7] A. Hemmer, R. Badonnel, and I. Chrisment, "A Process Mining Approach for Supporting IoT Predictive Security," in *Proceedings of the Network Operations and Management Symposium (NOMS 2020)*, April 2020.

[8] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[9] B. Dongen, A. Medeiros, H. Verbeek, A. Weijters, and W. Aalst, "The ProM Framework: A New Era in Process Mining Tool Support," vol. 3536, June 2005, pp. 444–454.